LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

CERT gouvernemental

GRAND DUCHY OF LUXEMBOURG
GOVCERT.LU

ACTIVITY REPORT
2012 | 2013

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

On 15th July 2011, the Council of Luxembourg Government approved the creation of a new governmental entity known as Computer Emergency Response Team of the Government of Luxembourg (hereafter GOVCERT.LU). GOVCERT.LU is responsible for handling cybersecurity incidents in Luxembourg's public sector institutions and critical private sector infrastructures, which are monitored by the Haut-Commissariat à la Protection Nationale (hereafter HCPN).

In its latest risk report for 2013 The World Economic Forum (WEF) has recognised cyber-attacks among the top global risks with the highest likelihood of occurrence. In fact, during the period 2012-2013 the Luxembourg´s public sector has been affected by several incidents which have had limited impact on information security. A number of threats were identified, which could have affected governmental infrastructures not only in Luxembourg but throughout the world. Among these incidents were "Red October", "APT1" and "MiniDuke".

Incidents are handled by the security analysts at GOVCERT.LU and categorised into several types according to their severity, attack type, complexity, impact and other relevant factors. Incident categorisation has enabled GOVCERT.LU to handle these issues in a more efficient manner, allowing them to keep a record of incident trends over time in order to refine the future protection strategy and measures.

GOVCERT.LU activities and services actually go beyond pure incident handling. The management has defined a strategic plan of short and medium-term measures to increase the preparedness of GOVCERT.LU towards cybersecurity. Such measures are integrated in GOVCERT.LU's agenda and will be fully deployed in the coming years and include proactive activities such as malware analysis, vulnerabilities management, development of security tools and training sessions to various stakeholders, playing an important role in making Luxembourg a "safer" place.

GOVCERT.LU is not a stand-alone organisation. It sustains an important role at national and international levels, having active cooperation on a day-to-day basis with many institutions such as HCPN and Centre des Technologies de l'Information de l'État (hereafter CTIE). It also strongly encourages collaboration with international agencies like European Network and Information Security Agency (hereafter ENISA) or other CERTs.

2. INTRODUCTION

Computer Emergency Response Teams (CERTs), also known as Computer Security Incident Response Teams (hereafter CSIRTs) are the key organisational instruments for Critical Information Infrastructure Protection (hereafter CIIP). Every country must have capabilities at hand to effectively and efficiently respond to information security incidents. CERTs act as primary security service providers for governments and citizens, as well as educating and raising awareness (more details on CSIRT activities in section 2.1).

This Computer Emergency Response Team of the Government of Luxembourg activity report (GOVCERT.LU) concludes / highlights:

- The main activities carried out by GOVCERT.LU which revolve around the handling of information security incidents at government infrastructural level;
- Key security trends and statistics of incidents handled during the period of April 2012 to September 2013;
- National and international collaborations with other governmental institutions, European CERTs, and other cybersecurity teams / forums.

This report is organised into three chapters:

Overview of GOVCERT.LU: Background information on GOVCERT.LU, its vision, and overview of its organisational structure and outlook of future steps.

State of Security: This chapter presents details about key security trends, statistics from recorded incidents and the regulatory context applicable to the European Union and specifically to Luxembourg.

Activity report: This section provides more insight into the activities of GOVCERT.LU beyond incident handling, such as malware analysis, development of security tools, national and international collaborations and key events organised.

Explanations of jargon and technical terms can be found in a glossary ("Additional Information" section) at the end of this report.

2.1 CSIRT main activities

A CSIRT is a service responsible for receiving, reviewing and responding to computer security incidents.

The size and structure of a CSIRT depends on the organisation it serves. CSIRTs can support public institutions, a country or even an entire region (e.g. the Japan Computer Emergency Response Team Coordination Center or the AusCERT for the Asia-Pacific area). A CSIRT can also be formed as an ad-hoc team, created to respond to a specific incident when the need arises.

A CSIRT can carry out both reactive and proactive functions to protect the critical assets of an organisation. There is no standard set of functions a CSIRT provides. Whatever services

it chooses to deliver, the objective must be based on the business goals of the constituent. Protecting critical assets is the key to success of both the organisation and the CSIRT.

CSIRTs help organisations to contain and to recover from computer security breaches and threats. This reactive function is called incident handling. Usually, it includes three main functions:

1. The incident reporting function enables a CSIRT to serve as a central point of contact for reporting local problems. All incident reports are collected in a single location where information can be reviewed.

2. The incident analysis function is used to determine trends and patterns of intruder activity and recommend corresponding preventative strategies to the organisation. Incident analysis also involves taking an in-depth look at an incident report or incident activity to determine the scope, priority and threat, along with researching possible response and mitigation strategies.

3. The incident response function can take many forms. A CSIRT may send out recommendations for recovery, containment or prevention to the organisation or perform those response steps itself.

A CSIRT's services may also include proactive functions. These types of services are related to security awareness training, intrusion detection, penetration testing, documentation or even software development. These proactive functions can help an organisation to not only prevent computer security incidents but also to reduce the time it takes to react to an incident.

The reactivity constitutes a critical consideration in assembling, maintaining and deploying an effective CSIRT. A rapid, accurately targeted and effective response can minimize the overall damage caused by a specific incident. Another important consideration involves the ability of the CSIRT to support law enforcement bodies in tracking down the perpetrators of an incident in order to effectively prosecute them.

3. OVERVIEW OF GOVCERT.LU

3.1 Background on GOVCERT.LU, vision and strategy

GOVCERT.LU mainly focuses on the new challenges that information and communication technologies offer today as Luxembourg heads towards becoming a global ICT player. With the aim of strengthening its existing entities for fighting cyber-attacks, the Council of the Luxembourg government approved the creation of two new governmental departments during a session held on 15th July 2011: the Luxembourgish Cyber Security Board and the governmental CERT (GOVCERT.LU).

GOVCERT.LU acts at both national and international levels to protect the Grand Duchy of Luxembourg against major cyber threats, to provide an attractive, secure and reliable environment for local businesses in Luxembourg, and to protect the privacy and fundamental rights of people in Luxembourg.

To fulfil its missions, GOVCERT.LU is mandated to cover classified and non-classified infrastructures, **to react and to coordinate in the event of incidents, to prevent and detect major incidents** and to improve coordination among governmental departments within the scope of incident handling and response.

GOVCERT.LU supports its constituency with a set of reactive and proactive services in the field of information / IT security and is authorised to handle and to address all types of information security incidents, which occur or threaten to occur, in the networks, systems and services that fall into its mandate.

Since GOVCERT.LU is still in its early years of operation, its services have been deployed gradually. At the moment GOVCERT.LU is significantly involved with incident handling, however its agenda includes services which will become more vibrant in the coming years. Some of these services including malware analysis, development of security tools and provision of training sessions are detailed in this report.

Message from GOVCERT.LU (Computer Emergency Response Team of the Government of Luxembourg)

“With an increasing dependency on information and communication technologies, the threats to which our citizens, businesses and critical infrastructures are exposed to are growing steadily. New technologies bring with them new opportunities, but also create many new risks. Cloud computing and mobile devices, coupled with new concepts like “bring your own device”, offer immense flexibility and have the potential to boost efficiency in many activities.

However, continued investment in cybersecurity is needed to minimise risk and to keep pace with new and emerging threats. As these threats emerge, cyber-attacks become more frequent. This is partly due to the growing number of potential victims and the profits available to the cyber attackers.

> Managing cyber incidents has become a necessity and has led to the creation of dedicated teams in order to achieve this task. Their aim is to rapidly restore the status quo and normal operational systems. Other activities include raising the awareness and understanding of cyber incidents. This allows for a better risk assessment to support and advise the government in making the right decisions in cyber-crime prevention and detection.
>
> In setting up the Governmental Computer Security Incidents Response Team, the Luxembourgish Government took an important decision in the fight against cyber-crime. ”
>
> *Patrick HOUTSCH – Managing Director GOVCERT.LU*

3.2 Overview of organisational structure and key members

GOVCERT.LU is operated by the State Ministry under the auspices of, and with authority delegated by a decision of the Council of Government dated of 15th July 2011. The GOVCERT.LU team is operated by dedicated IT security experts.

Since most of the proactive activities of GOVCERT.LU for handling cybersecurity threats will be deployed in the next years and the number of incidents handled by GOVCERT.LU is increasing over time additional IT security experts will be hired to support its activities.

3.3 Investing into organisational development

GOVCERT.LU is a newly established governmental institution in Luxembourg. Since its inception it has invested in setting up and building internal working procedures and system architecture. At this stage, GOVCERT.LU has contributed to an important number of policy documents at different maturity levels related to various internal processes (e.g. information disclosure policy, incident categorisation, incident reporting guidelines for constituency, call handling, collaborations, etc.).

From a system perspective, GOVCERT.LU has set up a fully featured system architecture embedding a complete set of back office applications as well as more specific business applications, such as a ticketing system and information centralisation and correlation databases. In order to enable an efficient collaboration with its constituency, GOVCERT.LU has defined a sustainable procedure to manage constituent information.

GOVCERT.LU follows an accepted Information Security Management System (ISMS) based on ISO 27000 series and a quality assurance approach since its establishment.

Furthermore, GOVCERT.LU is following SIM3 (Security Incident Management Maturity Model) as per the instructions of FIRST (Forum of Incident Response and Security Teams - further discussed below). Based on the SIM3 model, GOVCERT.LU aims to give its security or incident response a specific level of maturity. This will be achieved by focusing on organisation, human resources, processes and tools. Prevention, detection, and feedback as well as resolution is also included in this focus[1].

[1] **SIM3:** *Security Incident Management Maturity Model - SIM3 mkXV, Don Stikvoort: http://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf*

4. THE STATE OF SECURITY

4.1 Cyber-attacks are one of the top five global risks for 2013

According to the latest annual report from the World Economic Forum (WEF)[2], **cyber-attacks are one of the top five global risks likely to impact the planet over the coming years**.

The international organisation (WEF or another – if another it needs to be stated which) interviewed more than 460 experts from industry, government, academia and civil society to compile its global risks report.

The report examined 50 global risks across five categories – economic, environmental, geopolitical, societal and technological – to formulate its conclusions. It placed cyber-attacks 4th on a list of top five global risks in terms of likelihood (after 'severe income disparity', 'chronic fiscal imbalances' and 'rising greenhouse emissions').

Specific to technological risks, cyber-attacks represent the risk with the highest probability of occurrence and in combination with its high impact, it is considered as one of the top technological risks together with critical systems failure, massive incident of data fraud / theft and digital misinformation.

The following figure shows the top technological risks for 2013 in terms of impact and likelihood of occurrence, based on the WEF report.

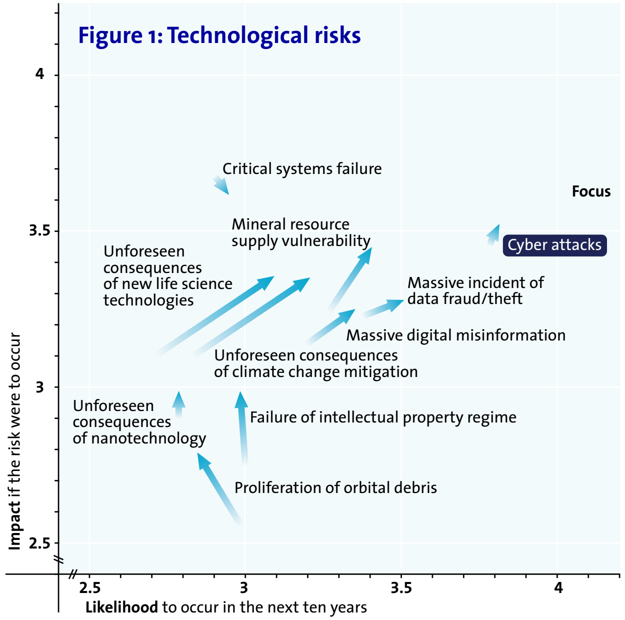


Figure 1: Technological risks

Despite the fact that the information security industry has been fighting cyber-attacks for several years, it is only now that WEF highlights cyber-attacks as a major threat at a global level. However, WEF recognises cyber-attacks as criminal or terrorist attacks that can be also state-sponsored or state-affiliated and organisations either in the private or public sector need to acquire a better understanding of the true levels of the associated risk.

[2] **Global Risks 2013**, *8th edition – World Economic Forum: http://www.weforum.org/reports/global-risks-2013-eighth-edition*

4.2 Overview of key security incidents

4.2.1 Malware at the heart of cyber-attacks

Malware (short for malicious software) is software used or created by attackers to disrupt computer operations, steal sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. It is a general term used to refer to a variety of forms of hostile or intrusive software.

The effects of malware have been such that it forced the adoption of protection measures by most personal users and companies.

In spite of the various protection measures applied by governmental institutions, companies and individuals, nobody can guarantee that malware can be detected and effectively eliminated. In fact, today's malware detection rate is below 100%. **Malware is always evolving and new threats appear on a daily basis across the globe challenging users of systems, antivirus companies and organisations fighting cybersecurity threats.** For GOVCERT.LU, a quick response to an incident is of vital importance for the cybersecurity of its constituency. For that purpose, GOVCERT.LU is continuously trying to improve its operations in incident handling by developing security tools, analysing malware and creating user awareness on key security events.

4.2.2 Advanced Persistent Threats

"Advanced Persistent Threats" or APT are cyber-attacks which are concentrated against a single target or group of targets and last until access is gained to the organisations IT environment. APT attacks are intended to remain "under the radar" for as long as possible to retrieve information. APTs usually create a backdoor in a vulnerable computer system (e.g. via the use of phishing emails) to gain access to a whole infrastructure where it can create new backdoors and collect and communicate information outside the organisation.

Through their intrusion detection activities, GOVCERT.LU is observing many attacks of this kind and believes that such attacks will become more frequent in the future.

The Red October Case

Red October (identified as "Rocra") is a targeted attack campaign that has been going on for at least five years. It has infected hundreds of victims around the world in eight main categories: Government, Diplomatic / Embassies, Research institutions, Trade and Commerce, Nuclear / Energy Research, Oil and Gas companies, Aerospace and Military. It is quite possible that there are other targeted sectors which have yet to be discovered or that have been attacked in the past. In Luxembourg, Red October has primarily affected governmental institutions.

This campaign primarily targets countries in Eastern Europe, former USSR Republics, and countries in Central Asia, although victims can be found everywhere, including Western Europe and North America.

The main objective of the attackers is to gather sensitive documents from the compromised organisations, which include geopolitical intelligence, credentials to access classified computer systems, and data from personal mobile devices and network equipment[3].

[3] **Red October – Kaspersky Lab**: *http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide*

In Luxembourg, Red October had a limited impact on governmental ICT systems. A detailed analysis of the affected system by GOVCERT.LU showed that the attack could not be considered as unusually severe.

The APT1 Case

It is believed that APT1 is a single organisation of operators that has conducted a cyber-espionage campaign against a broad range of victims since at least 2006. APT1 is alleged to be one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen.

Information stolen by the group includes manufacturing procedures, business plans, policy positions and analysis, emails of high-ranking employees, user credentials, and product development and use. However, there is no "direct evidence" about who ends up receiving that information, or how all that data is processed into a usable form[4].

The MiniDuke Case

In February 2013, Kaspersky Lab's team of experts published a new research report on a series of security incidents involving the use of the then discovered PDF exploit in Adobe Reader (CVE-2013-6040) and a new, highly customised malicious program known as MiniDuke. The MiniDuke backdoor was used to attack multiple government entities and institutions worldwide during February 2013. Kaspersky Lab, in partnership with the CrySys Lab, analysed the attacks in detail and published their findings.

According to their findings, a number of high profile targets have already been compromised by the MiniDuke attacks, including government departments in Ukraine, Belgium, Portugal, Romania, Czech Republic and Ireland. In addition, a research institute, two think tanks, and a healthcare provider in the United States were also compromised, as was a prominent research foundation in Hungary[5].

GOVCERT.LU confirmed that there have been victims of such a cyber-attack among its constituency. A detailed analysis revealed that the incident was of limited impact and involved only a very small number of governmental workstations. In the end, no critical systems have been affected and appropriate safeguarding measures have been deployed.

4.2.3 Oracle Java CVE-2013-0422

On 11th January 2013 a vulnerability notification was published by GOVCERT.LU to increase public awareness of a highly critical vulnerability in Oracle Java (CVE-2013-0422) affecting the Java plugin for Internet Explorer web browser. At the time of notification an update that could fix this issue was not yet available.

This vulnerability might be remotely exploited without authentication (i.e. without the need for a username and password). To be successfully exploited, an unsuspecting user running an affected release in a browser will need to visit a malicious web page that exploits these vulnerabilities. Successful exploits can impact the availability, integrity, and confidentiality of the user's system[6].

---

[4] **APT1** - *Exposing One of China's Cyber Espionage Units - http://intelreport.mandiant.com*
[5] **Miniduke** - *Kaspersky Lab - http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_MiniDuke_a_New_Malicious_Program_Designed_for_Spying_on_Multiple_Government_Entities_and_Institutions_Across_the_World*
[6] **Oracle Security Alert** *for CVE-2013-0422: http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html*

4.3 The regulatory context

4.3.1 A regulatory baseline

The Grand-Ducal decree of July 30th 2013 lays down the legal basis that determines GOVCERT.LU's organisation and activities.

On 6th September 2013 and after more than a year of operational activities at GOVCERT.LU, this decree has been published in the Luxembourgish memorial with the aim to confirm the decision of the Council of Luxembourg Government and by doing so, giving a stronger legal baseline to the Luxembourgish Governmental CSIRT[7].

4.3.2 GOVCERT.LU has become an accredited member of Trusted Introducer

On 8th June 2012, GOVCERT.LU's status was updated to an accredited member by Trusted Introducer (TI). This is an important step for a CSIRT towards a successful integration into the European CSIRT community.

The Trusted Introducer represents a backbone for the Security and Incident Response Team community in Europe. The TI lists, accredits and certifies teams, and provides them with a well-balanced set of trusted security services[8].

4.3.3 Internal procedures in handling sensitive information

GOVCERT.LU regards highly the importance of operational cooperation and information sharing between Computer Emergency Response Teams and other organisations which may contribute to or make use of its services.

GOVCERT.LU will share information whenever this may assist the community in resolving or preventing security incidents whilst appropriate measures will be taken to protect the identity of victims. Sensitive information remains protected in accordance with relevant regulations and policies within Luxembourg. In particular, GOVCERT.LU strictly respects sensitivity labelling of information adopted by the referring entity.

4.3.4 Guidelines to support the operation of European CERTs

The successful creation and operation of CERTs / CSIRTs depends on a number of factors. A lot of mistakes can be made, especially in early phases that are difficult or impossible to mitigate later. For that purpose, ENISA provides a series of guidelines that aim at helping EU Member States, but also other stakeholders, to efficiently establish and operate CERTs / CSIRTs. The guidance provided by ENISA has been created in cooperation with experts in this field, who have many years of hands-on experience[9].

When GOVCERT.LU was established its management team followed the guidelines provided by ENISA which describe the processes of setting up a CSIRT (e.g. CSIRT strategy planning, business plan development, etc.). At the operational level, GOVCERT.LU also follows "running" guidelines on successful CSIRT operation, exercise and training material, baseline/ minimum capabilities of a CSIRT, incident management and other guidelines.

4.3.5 Best practice guidelines established by FIRST

FIRST is a global forum that brings together a variety of computer security incident response teams from government,

[7] **The Grand-Ducal decree of July 30th 2013:** *http://www.legilux.public.lu/leg/a/archives/2013/0161/a161.pdf#page=2*
[8] **Trusted Introducer**: *http://www.trusted-introducer.org/*
[9] **Support for CERTs / CSIRTs – ENISA**: *http://www.enisa.europa.eu/activities/cert/support*

commercial, and educational organisations. It aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides other services, such as access to an up-to-date best practice guide library. The intention is to assist FIRST team members and the public in configuring their systems securely by providing configuration templates and security guidelines. Such guidelines are important as it is a complicated and time-consuming task even for experienced system administrators to know what a reasonable set of security settings is for any operating system. GOVCERT.LU follows these guidelines whenever possible in order to ensure that strict IT security measures are applied[10].

4.3.6 Network and Information security (NIS) measures across the EU

The European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, has published a proposed Directive on network and information security (NIS) which should be implemented by all Member States when it is adopted by the Council and European Parliament.

The aim of the proposed Directive is to ensure a high common level of network and information security. This means improving the security of the Internet and the private networks and information systems underpinning the functioning of European societies and economies. This will be achieved by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures such as energy, transport and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the relevant national authorities[11].

Among other requirements, this new proposal requires Member States to set up a minimum level of national capabilities by establishing competent authorities for NIS, setting up Computer Emergency Response Teams, and adopting national NIS strategies and cooperation plans.

With the creation of its governmental CERT, the Luxembourgish Government has already taken an important step to comply with what might very soon become a legal requirement.

Message from SnT (Interdisciplinary Centre for Security, Reliability and Trust – University of Luxembourg)

“GOVCERT.LU is essential to Luxembourg’s economic dynamics: Modern-day information and communication technology’s impact on our lives, our work, and our leisure and consumer behaviour is increasing. Thus, ICT security, reliability and trust are highly important prerequisites for a sustainable development in this field. GOVCERT.LU ensures that Luxembourg is optimally positioned and protected against cyber-attacks: It is an essential instrument in offering citizens and industry

[10] **FIRST**: *http://www.first.org/*
[11] **Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** *concerning measures to ensure a high common level of network and information security across the Union - 2013/0027 (COD) – European Commission: http://eeas.europa.eu/policies/eu-cyber-security/*

> an attractive and trustworthy ICT environment. Security research is needed to assure Luxembourg's role as an international leader in this sector. I look forward to developing deeper collaboration between GOVCERT.LU and SnT to realise this goal. ”
>
> *Björn OTTERSTEN – Director of SnT - "Digital Champion"*

4.4 Incidents handled by GOVCERT.LU are recorded and monitored

An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security (ISO 27000 series). Incidents are processed through a ticketing system by the responsible operator. A unique ticket "ID" number is assigned to every incident and its details and status are monitored even after the incident is completely resolved.

GOVCERT.LU has categorised incidents using different variables including attack complexity, attack type, victim sector, incident impact, incident category, and used vulnerabilities. Such detailed categorisation enables GOVCERT.LU to be more proactive and to identify future trends out of previous incidents and to also take accurate decisions on handling incidents. A more detailed description of incident categories can be found in the glossary.

4.5 Incidents handled by GOVCERT.LU

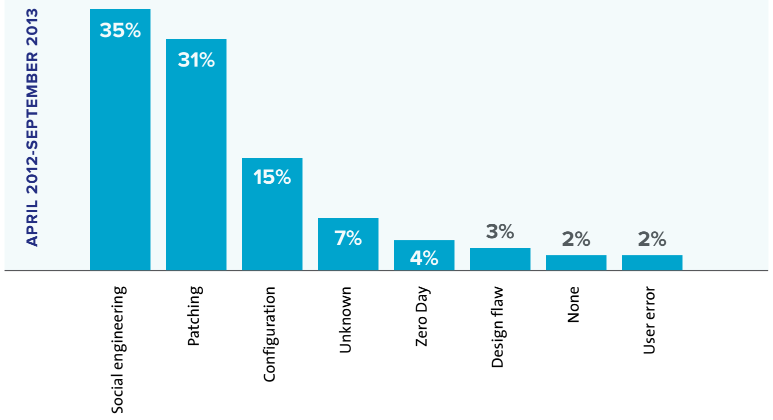
GOVCERT.LU handled several hundred incidents for the period of April 2012 to September 2013. These incidents include all the cases handled by GOVCERT.LU including incidents that were handled by its analysts but which impacted victims outside its user group. It is important to note that these figures do not include events such as investigations or notifications.

GOVCERT.LU has set up an incident control process by which the first trends on information security can already be shown. A list of key statistics has been prepared and presented below, showing useful information based on the categorisation of incidents provided above.

However the trends are not necessarily sustainable because the statistical robustness is only at a developing stage.

4.5.1 Exploited vulnerabilities

Figure 2: Used vulnerabilities



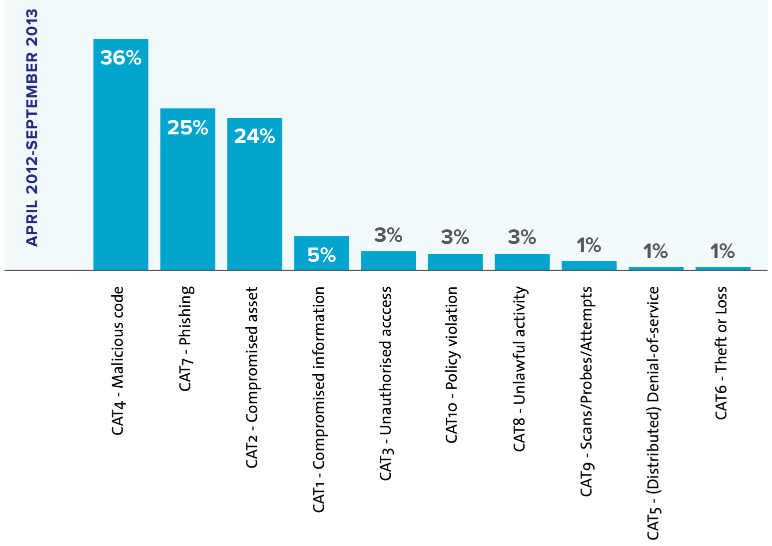
31% of the vulnerabilities used in incidents handled by GOVCERT.LU have been classified as "patching", meaning that those attacks would not have been successful on a fully patched system. **Such incidents can be avoided by adopting an effective patching policy.**

35% of the vulnerabilities have been classified as "social engineering". This in return shows how important it is to **raise awareness and train people with regards to the social engineering aspect of cyber-attacks.**

Very few incidents are related to poor design unknown or zero day vulnerabilities.

4.5.2 Incident categories

Figure 3: Incident categories

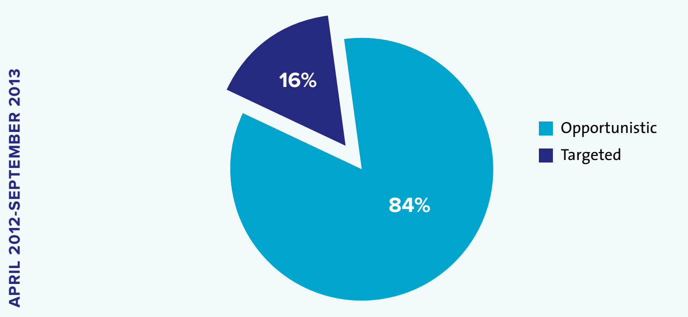


Very few incidents had an impact on information (e.g. documents, databases, credentials) as only 5% of the handled cases have been related to compromised information category.

On the other hand, it can be shown that many incidents were related to the use of malicious code (36%) as well as of phishing techniques (25%). In 24% of the cases an asset had been successfully compromised by the attacker. Finally, one may notice the very few cases of denial-of-service attacks.

4.5.3 Targeted attacks

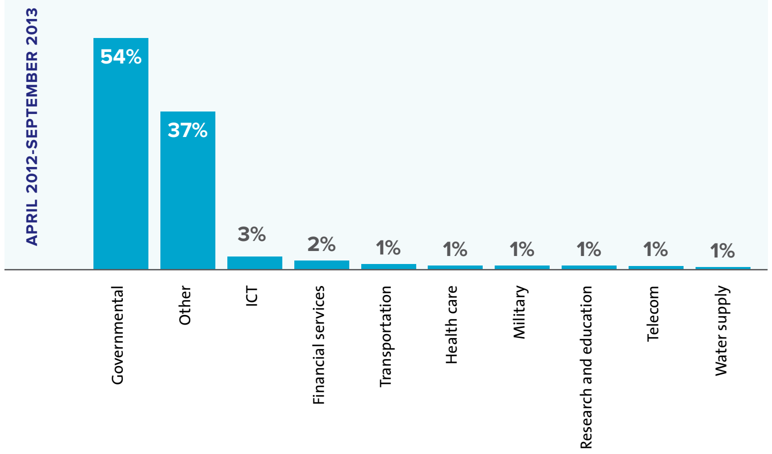
Figure 4: Share of targeted / opportunistic attacks



As this chart shows, most cyber-attacks are not specifically targeted against GOVCERT.LU's constituency. In fact **the large majority of handled incidents are related to opportunistic attacks (84%) whereas the targeted attacks account for only 16% of the cases.**

4.5.4 Victim sector

Figure 5: Victim sector

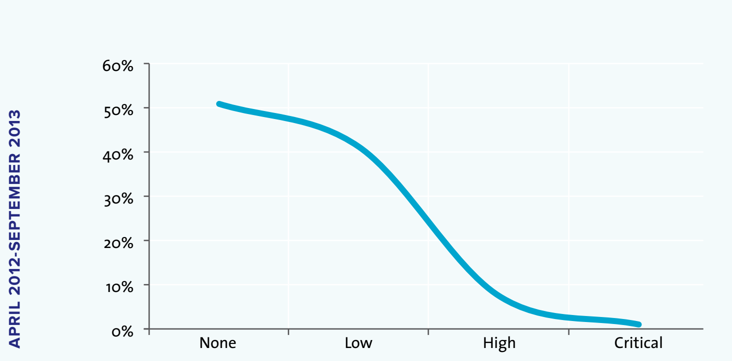


Most of the incidents handled by GOVCERT.LU have occurred in governmental institutions. This does not necessarily mean that incidents are rare in all other sectors, but so far only a few have been reported to GOVCERT.LU.

In the future, GOVCERT.LU is planning to ensure more active collaborations with other organisations in order to better handle incidents in various other sectors.

4.5.5 Incident impact

Figure 6: Real incident impact

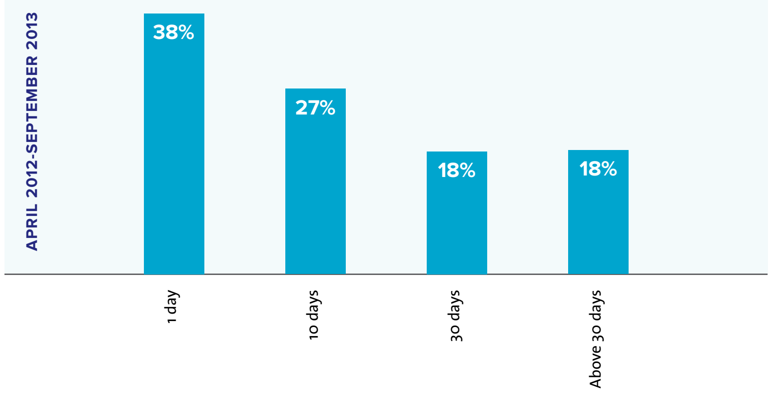


The above figure shows the impact an incident has on GOVCERT.LU's constituency only. It is essential to note that this figure does not account for the possible impact an incident could have outside GOVCERT.LU's scope.

It is noted that the majority of the incidents handled by GOVCERT.LU are of limited impact to its constituency.

4.5.6 Days to resolve incidents since identification

Figure 7: Days to resolve incidents since identification

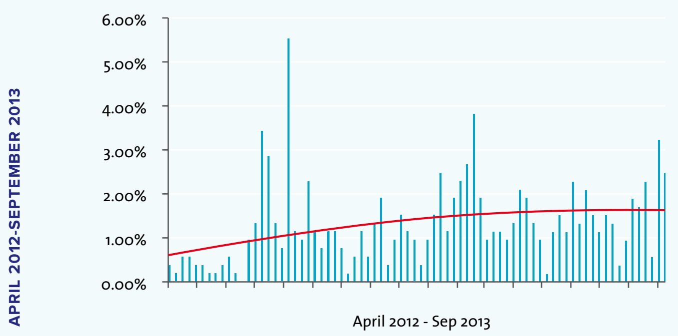


This specific chart can be considered as a performance indicator for GOVCERT.LU on resolving incidents.

The figure shows how many days it takes GOVCERT.LU security analysts to resolve an issue that has been identified and recorded. Most of the incidents (about 65% of the total incident population) are resolved within 10 days following their notification to or detection by GOVCERT.LU.

4.5.7 Number of incidents per week

Figure 8: Number of incidents per week



The red trendline shows a slight increase of incidents handled over time. This trend is likely to keep on growing in the coming years until GOVCERT.LU activities are fully deployed and its constituency awareness has been fully set up.

4.6 New technologies and future challenges

Innovation is the secret weapon that helps businesses keep pace with change. In order to adapt to change, businesses need to explore, implement and refine new technologies to continue growing and evolving, particularly as threats evolve and risks grow. But the few technologies that help propel a business forward are the same ones that create new risks. New technologies open up tremendous opportunities for organisations, but the information security function needs to pay particular attention to associated risks and manage them appropriately.

4.6.1 Cloud computing

Cloud computing can enable many organisations to increase their IT use by becoming more strategy-focused and less operations-focused. Cloud-based services are nimble and adaptive, increasing the capability to read and react to changing marketplace conditions by responding to customer needs and competitors' actions.

Although there is no doubt that cloud computing appears to be well on its way to mainstream adoption, concerns over security and privacy are being voiced. Effectiveness and efficiency of traditional information security and protection mechanisms are indeed questioned as cloud computing brings a new working model along with its adoption. On the privacy side, there is the threat that personally identifiable information stored in the cloud can be breached more easily than if stored in-house.

Cloud computing requires an entirely new security governance model and process. Factors that could accelerate the resolution of security and privacy issues associated with cloud computing adoption are leading practices, standards and cloud-specific regulation of security / privacy, all of which are slowly emerging from several regions around the world[12].

4.6.2 Mobile technology

Technology advancement and the associated business benefits have vastly increased adoption rates of mobile technology. Tablet computer usage in business activities has more than doubled since 2011. As the mobility of today's workforce continues to grow, the phrase "out of the office" becomes less relevant and the dramatic increase in the flow of informa-

[12] **Cloud computing:** *http://web.mit.edu/newsoffice/topic/cloud-computing.html*

tion in and out of an organisation becomes more difficult to control. Organisations recognise the need to do more. They are beginning to educate themselves about the capabilities and design of the mobile device security software products that are available on the market. Nevertheless, **the adoption of security techniques and software in the fast-moving mobile computing market is still low**. Encryption techniques are used only by few organisations. That clearly shows that the number of incidents as a result of using mobile technology will increase over time.

4.6.3 SCADA (Supervisory Control and Data Acquisition)

SCADA are control systems used to monitor and control industrial and manufacturing processes. These systems are used by a broad range of industries. SCADA systems basically collect relevant information through various kinds of sensors, which is then used to analyse events and trigger actions if required. The complexity of such systems ranges from simple to extremely complex depending on the company size and its business requirements.

SCADA software, used for industrial control mechanisms in utilities, airports, nuclear facilities and manufacturing plants is increasingly becoming a target for attackers looking to exploit what appear to be growing numbers of vulnerabilities – giving rise to fears that critical infrastructure may be at risk. **With SCADA software being primarily responsible for critical operations and national infrastructures, an attack of this nature could not only result in the loss of data, but could also cause damage to physical assets and in some scenarios, the loss of life**.

For now, cyber-attacks on SCADA systems are rare when compared to the number of incidents involving web applications or corporate IT networks, but the threat they pose is extremely severe. As such, security must be updated[13].

4.6.4 Distributed Denial-of-service (DDoS)

Distributed denial-of-service attack (DDoS attack) is a technique where hundreds or thousands of computer systems simultaneously conduct repeated queries to a victim's servers. As a result the volume of network traffic generated by this kind of attack is such that the targeted systems become unavailable and legitimate business cannot be conducted anymore. Some companies whose servers have been brought down using these denial-of-service attacks have reportedly lost up to millions of Euros per day[14].

There are two common ways to perform DDoS attacks. On one hand, attackers can force the targeted system to consume its resources so that it can no longer provide its service. On the other hand, attackers can block the communication means between legitimate users and the target so that the latter can no longer communicate effectively.

The DDoS phenomenon started in 2003 when a number of online companies, including an online betting site, were attacked. Since then, DDoS attacks have become increasingly common. **Online services should evaluate the opportunity to adopt measures against such attacks**.

[13] **Critical infrastructure at risk from SCADA vulnerabilities:** *http://www.infosecurity-magazine.com/view/29544/critical-infrastructure-at-risk-from-scada-vulnerabilities-/*
[14] **Denial-of-service attack:** *http://www.cert.org/tech_tips/denial_of_service.html*

5. ACTIVITY REPORT

5.1 Report on key events organised and supported

Participation in Cyber Europe 2012

On 4th October 2012 more than 500 cybersecurity professionals across Europe including GOVCERT.LU, HCPN and CIRCL (Computer Incident Response Center Luxembourg) participated in Cyber Europe 2012, the second pan-European Cyber Exercise organised by the European Network and Information Security Agency (ENISA).

Cyber Europe 2012 had three objectives:

1. Test the effectiveness and scalability of mechanisms, procedures and information flow for public authorities' cooperation in Europe;

2. Explore the cooperation between public and private stakeholders in Europe;

3. Identify gaps and challenges on how large-scale cyber incidents could be handled more effectively in Europe.

The exercise scenario revolved around large-scale cyber incidents in Europe, which affected all participating countries. Fictional adversaries joined forces in a massive cyber-attack against Europe, mainly through (distributed) Denial-of-service (DoS) attacks against public electronic services. The affected services were online e-government and financial (e-banking, etc.) services.

Cyber incidents challenged the public and private sector participants, triggering a need for cross-country cooperation. Players received information on the scenario (injects) via emails, and had to collaborate using standard procedures and structures in order to assess the situation and agree upon a course of action.

Cyber Europe 2012 produced a series of key findings regarding cooperation on national and international levels. The cyber exercises are summarised below:

- Playing countries took cybersecurity incidents very seriously, responding to the challenges by escalating issues to their national crisis response cells and / or activating national crisis structures.

- Cyber Europe 2012 helped to build trust between countries. **Trust is the key for successful and timely mitigation activities during real cyber-crises**. The exercise has fostered both new and existing relationships.

- Cyber Europe 2012 has proven extremely useful for testing national contingency measures and levels of preparedness[15].

[15] **Cyber Europe 2012, key findings and recommendations, ENISA:** *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report*

5.2 Tools and Methods used by GOVCERT.LU to support incident handling

5.2.1 Sharing of information

In the world of CERTs, the exchange of information related to cyber incidents is of great importance. Indeed, incident management is often based on information exchanged between CERTs at national and international level. Therefore it is essential to have the necessary exchange of information and also to implement procedures for creating effective collaboration between contacts. The exchange of information relates to incident reports, malware analysis, IP addresses and malicious Internet sites and vulnerabilities and artefacts of any kind (e.g. viruses, trojans, etc.).

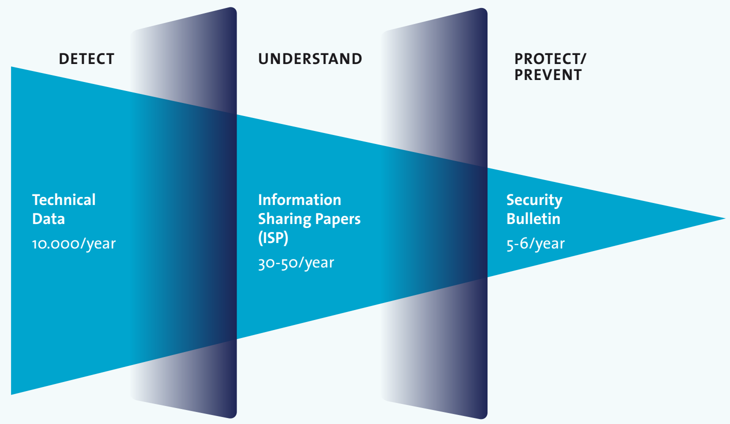
GOVCERT.LU shares incident information with its constituency and third parties at different levels. Technical data including indicators of compromise (IOC) (e.g. URLs, domain names, IPs, ASN, file hashes, Filenames, Network traffic signatures, etc.) as well as malware samples and vulnerability notifications are shared on a regular basis.

According to the importance of the incidents detected, Information Sharing Papers (ISP) can be issued in order to get more insight into specific incidents. ISPs typically contain a richer set of information such as malware reversing details.

If any of these incidents are of significant importance, appropriate protection and prevention measures should be set up. GOVCERT.LU will then issue a security bulletin including in-depth impact analysis, time line information, attack profile as well as recommendations.

The graph below shows the differences among the different types of sharing information used by GOVCERT.LU.

Figure 9: Information sharing funnel



5.2.2 Malware analysis

A "Lab" is operated by GOVCERT.LU security analysts where they can safely execute and inspect advanced malware. Analysts use this secure environment to test, replay, characterise, and document advanced malicious activities.

Malware examination can be achieved either through static or dynamic analysis. Static analysis involves investigation of malware in a safe environment and without real code execution. However, in order to better understand the behaviour of certain malware, dynamic analysis is required. Dynamic analysis is a method used for determining malware's execution behaviour by running and observing the malicious code in a protected environment.

5.2.3 Development of security tools

Security analysts at GOVCERT.LU are involved in the development of security tools that further improve GOVCERT.LU efficiency in handling incidents. Such tools include passive DNS database, automated log parsing tools, artefact handling database, data visualisation systems, open source intelligence tracker, system cloning and forensics tool box. Whenever possible, GOVCERT.LU tries to make these developments available to the community.

5.2.4 Training sessions / workshops

GOVCERT.LU will provide a series of training sessions or workshops for public sector institutions and other non-governmental infrastructures to help them handle incidents and improve future collaborations.

Through these training sessions, GOVCERT.LU will inform various stakeholders about available services, provides statistics regarding cyber-crime and incidents reported in the European Union, explains the collaboration of GOVCERT.LU with other institutions in fighting cyber-crime and provides typical examples of different type of incidents (e.g. malicious code, phishing, compromised asset, etc.).

Furthermore, GOVCERT.LU will provide information about the different ways that are available for system users to report incidents and how certain organisations can register with GOVCERT.LU to enable better performance in handling incidents.

5.2.5 Quality control

GOVCERT.LU gives high importance on the quality of services provided. Besides the internal monitoring of the quality and performance on incident handling by the security analysts, GOVCERT.LU undertakes customer satisfaction surveys on a regular basis.

GOVCERT.LU requests and receives feedback from selected incident victims in order to further improve its services for the future.

5.3 National and international collaborations

GOVCERT.LU strongly collaborates with other governmental institutions with the objective to enhance IT and network security in Luxembourg's public sector and critical infrastructures.

5.3.1 Haut-Commissariat à la Protection Nationale

HCPN is responsible for managing crisis situations in Luxembourg and protecting the citizens of Luxembourg from threats that could potentially lead to a crisis. Cyber-crime is currently one of HCPN's hot topics and it works together with GOVCERT.LU in developing a national cybersecurity plan.

A strong relationship exists between HCPN and GOVCERT.LU at various levels. These include the reporting of high risk incidents that are further assessed by HCPN as well as the definition and protection of critical infrastructures in Luxembourg.

Critical infrastructure corresponds to all facilities, networks, services, systems or even sectors of vital importance for

which the destruction, damage, interruption of function or disclosure would threaten national security, national economy, public health, and safety of the population or governmental operations.

According to a new national law (currently at draft stage) based on the European Directive 2008/114/EC, critical infrastructures operating within the borders of Luxembourg should be identified and protected. In this context, the owners and operators of critical infrastructures may be invited to take the necessary measures to improve resilience and facilitate crisis management. The proposed scheme introduces additional administrative sanctions in case of non-compliance with the new law and adapts several other legal texts.

Message from HCPN (Haut-Commissariat à la Protection Nationale)

“Since its beginning, GOVCERT.LU has already had considerable impact on several levels in the cyber landscape in Luxembourg and beyond. While building up the capacities on the classical CERT day-to-day business, it has established itself as a prime contact for policy makers and has an important role to play in national CIIP.”

Paul RHEIN – Conseiller-Informaticien 1ère classe

5.3.2 Cyber Security Board

As a member of the Cyber Security Board (CSB), GOVCERT.LU contributes to the creation and maintenance of Luxembourg's national cybersecurity strategy. Furthermore GOVCERT.LU supports the CSB with its consultancy and expertise services. Drafting technical expertise documents or chairing working groups of the CSB are two examples on how GOVCERT.LU supports the national Cyber Security Board.

5.3.3 Centre des Technologies de l'Information de l'État

CTIE has been established in 2009 by the Luxembourg Government to better meet the challenges of the information society and support the generalisation of electronic exchanges within the public sector.

The Security and Audit Division (DSA) of CTIE is a strategic partner for GOVCERT.LU. DSA provides to the security analysts of GOVCERT.LU the necessary technical information and data that enable GOVCERT.LU to detect many cyber incidents in near real time without user intervention.

Message from CTIE (Centre des Technologies de l'Information de l'État)

“CTIE and GOVERT.LU collaborate on a daily basis regarding incident handling. The security analysts of GOVCERT.LU have the right technical skills to detect and resolve cybersecurity threats affecting governmental institutions. It's a highly motivated team of young professionals and we are benefiting from their reliability. We are looking forward to intensifying our collaboration in the future.”

Manuel PICCO - Chargé d'études-informaticien principal

5.3.4 TF-CSIRT

GOVCERT.LU has been a member of the Task Force for Computer Security Incident Response Teams (TF-CSIRT) since its inception. A presentation of GOVCERT.LU was held at the task force meeting on 22nd September 2011. TF-CSIRT promotes collaboration and coordination between CSIRTs in Europe and neighbouring regions, while liaising with relevant organisations at a global level and in other regions.

TF-CSIRT provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination. It maintains a system for registering and accrediting CSIRTs, as well as certifying service standards.

The task force also develops and provides services for CSIRTs, promotes the use of common standards and procedures for handling security incidents, and coordinates joint initiatives where appropriate. This includes the training of CSIRT staff and assisting in the establishment and development of new CSIRTs.

The task force further liaises with FIRST, ENISA and other regional CSIRT organisations, as well as defence and law enforcement agencies[16].

5.3.5 FIRST

GOVCERT.LU is participating in events and meetings organised by FIRST which is the premier organisation and recognised global leader in incident response. It consists of a network of individual computer security incident response teams that work together voluntarily to deal with computer security problems and their prevention. These teams represent governments, law enforcements, academia, the private sector, and other organisations as determined by the Steering Committee.

[16] **Trans-European Research and Education Networking Association (TERENA) - TF-CSIRT:** *http://www.terena.org/activities/tf-csirt/*

6. GLOSSARY

APT1: Advanced persistent threat 1 (name given to a cyber-crime organisation by security company Mandiant).

CCG: Centre de Communications du Gouvernement (Luxembourg).

CIRCL: Computer Incident Response Center Luxembourg.

CSIRT: Computer Security Incident Response Team.

CTIE: Centre des Technologies de l'Information de l'État.

Cyber Security Board (CSB): The Cyber Security Board of Luxembourg has the mission to develop and maintain a national strategic plan against cyber-attacks and ensure the proper execution of this plan.

DDoS: Distributed Denial-of-service attack.

ENISA: European Network and Information Security Agency.

European Directive (2008/114/EC): Council Directive 2008/114/EC of 8th December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

FIRST: Forum of Incident Response and Security Teams.

GOVCERT.LU: Computer Emergency Response Team of the Government of Luxembourg.

HCPN: Haut-Commissariat à la Protection Nationale.

ICT: Information and Communication Technology.

Incident: A single or a series of unwanted information security events that have a significant probability of compromising business operations or threatening information security.

Incidents categories:

- CAT 1 – Compromised information: Successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
- CAT 2 – Compromised asset: Compromised host (root account, Trojan, root kit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
- CAT 3 – Unauthorised access: In this category an individual (internal or external) gains logical or physical access without permission to a national or local network, system, application, data, or other resource.
- CAT 4 – Malicious code: Malicious software (e.g. virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
- CAT 5 – (Distributed) Denial-of-service: An attack that successfully prevents or impairs the normal authorised functionality of networks, systems or applications by exhaust-

ing resources. This activity includes being the victim or participating in the DoS.

- CAT 6 – Theft or loss: Theft or loss of sensitive equipment (Laptop, hard disk, media etc.) belonging to the organisation.

- CAT 7 – Phishing: Use of fraudulent computer network technology to entice an organisation's users to divulge important information, such as obtaining users' bank account details and credentials by deceptive emails or fraudulent web site.

- CAT 8 – Unlawful activity: Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely to involve law enforcement, Global Investigations, or Loss Prevention.

- CAT 9 – Scans / Probes / Attempted access: This category includes any activity that seeks to access or identify an organisation computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial-of-service.

- CAT 10 – Policy violations: Deliberate violation of InfoSec policy, such as:

    - Inappropriate use of corporate asset such as computer, network, or application.

    - Unauthorised escalation of privileges or deliberate attempt to subvert access controls.

ISMS: Information Security Management System.

ISP: Information Sharing Papers.

Malware: Software used or created by attackers to disrupt computer operation, steal sensitive information, or gain access to private computer systems.

NIS: Network and Information Security.

Incident impact

- Critical: Incidents with a very high impact on the attacked organisation and where special and immediate response is required. Such incidents can lead to a potential crisis situation in Luxembourg, high ranking governmental officials may be contacted for further action and the situation is continuously monitored by GOVCERT.LU and other related parties.

- High: Incidents of high impact that require an immediate treatment, however the probability of such incidents to affect national security and lead to a crisis situation is limited.

- Low: Incidents of low or medium impact. These incidents are usually resolved by GOVCERT.LU without any additional support from other external parties. The majority of incidents fall into this category.

- None: Incidents that have no real impact for the users of the affected systems. Such incidents are frequent and represent a high portion of the total incidents handled by GOVCERT.LU.

SB: Security bulletin.

SCADA: Supervisory Control and Data Acquisition.

TF-CSIRT: Task Force for Computer Security Incident Response Teams.

TI: Trusted introducer is the trusted backbone of the Security and Incident Response Team community in Europe. The TI lists, accredits and certifies teams, and provides them with a well-balanced set of trusted security services.

Traffic Light Protocol (TLP): It was created to encourage greater sharing of sensitive information. It is a set of designations used to ensure that sensitive information is shared with the correct audience.

Vulnerabilities:

- **Patching**: This means that a patch for the used vulnerability was available. Therefore the incident could have been prevented if a patching policy was applied.

- **Zero day**: A zero-day attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability. This means that the developers have had zero days to address and patch the vulnerability. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability. Incidents exploiting this type of vulnerabilities are difficult to prevent.

- **Social**: This means that the attack used the nature of mankind by manipulating people into performing actions in order to be effective. Social engineering, in the context of security, is the art of manipulating people into performing actions or divulging confidential information. This is a type of confidence trick for the purpose of information gathering, fraud, or computer system access.

- **Configuration**: This vulnerability category refers mainly to a wide variety of server configuration problems that can plague the security of a web site. These include:

  - Server software flaws or miss-configurations that permit directory listing and directory traversal attacks.

  - Unnecessary default, backup, or sample files, including scripts, applications, configuration files, and web pages.

  - Improper file and directory permissions, etc.

- **Design flaw**: Insufficient input data validation or weakly designed security concepts. Such flaws are usually identified at a later stage during the operation of the specific software and can contribute to or cause a system failure or erroneous human decision.

- **User error**: These vulnerabilities refer to incidents that involve user errors. This includes loss of equipment or removable media and choosing weak passwords.

- **None**: Through analysis it was not possible to determine which vulnerabilities were used.

WEF: World Economic Forum.

7. REFERENCES

- SIM3: Security Incident Management Maturity Model - SIM3 mkXV, Don Stikvoort: http://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf
- Global Risks 2013, 8th edition – World Economic Forum: http://www.weforum.org/reports/global-risks-2013-eighth-edition
- Red October – Kaspersky Lab: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide
- APT1 - Exposing One of China's Cyber Espionage Units: http://intelreport.mandiant.com
- Miniduke - Kaspersky Lab: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_MiniDuke_a_New_Malicious_Program_Designed_for_Spying_on_Multiple_Government_Entities_and_Institutions_Across_the_World
- Oracle Security Alert for CVE-2013-0422: http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html
- The Grand-Ducal decree of July 30th 2013: http://www.legilux.public.lu/leg/a/archives/2013/0161/a161.pdf#page=2
- Trusted Introducer: http://www.trusted-introducer.org/
- Support for CERTs / CSIRTs – ENISA: http://www.enisa.europa.eu/activities/cert/support
- FIRST: http://www.first.org/
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union - 2013/0027 (COD) – European Commission: http://eeas.europa.eu/policies/eu-cyber-security/
- Cloud computing: http://web.mit.edu/newsoffice/topic/cloud-computing.html
- Critical infrastructure at risk from SCADA vulnerabilities: http://www.infosecurity-magazine.com/view/29544/critical-infrastructure-at-risk-from-scada-vulnerabilities-/

- Denial-of-service attack:
  http://www.cert.org/tech_tips/denial_of_service.html

- Cyber Europe 2012, key findings and recommendations, ENISA:
  http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report

- Trans-European Research and Education Networking Association (TERENA) - TF-CSIRT:
  http://www.terena.org/activities/tf-csirt/